IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF ILLINOIS
EASTERN DIVISION

In re: Clearview AI, Inc. Consumer Privacy Litigation	)	Case No. 1:21-cv-00135
	)	Hon. Sharon Johnson Coleman

CLEARVIEW DEFENDANTS' MEMORANDUM OF LAW IN SUPPORT OF THEIR MOTION TO DISMISS THE CONSOLIDATED CLASS ACTION COMPLAINT

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Defendants Clearview AI, Inc. ("Clearview"), Hoan Ton-That, Richard Schwartz, Rocky Mountain Data Analytics LLC ("Rocky Mountain"), and Thomas Mulcaire (collectively, the "Clearview Defendants") respectfully submit this memorandum of law in support of their motion to dismiss the Consolidated Class Action Complaint (Dkt. 29) (the "Complaint").

INTRODUCTION

Plaintiffs' claims against the Clearview Defendants under the Illinois Biometric Information Privacy Act ("BIPA"), 740 ILCS 14/15(c) and various other states' laws should be dismissed with prejudice for multiple, independent reasons.

At the outset, the Complaint should be dismissed as to the individual defendants and Rocky Mountain because Plaintiffs fail to state a claim against them. The individual defendants cannot be held liable for their conduct as officers and employees of Clearview, and the Complaint fails to allege any fraud permitting the Court to pierce the corporate veil. For the same reason, Plaintiffs fail to allege any basis for piercing the veil between Clearview and Rocky Mountain.

The Complaint fails as a matter of law as to all the Clearview Defendants because Plaintiffs improperly attempt to apply BIPA to Clearview's out-of-state conduct in violation of Illinois' extraterritoriality doctrine. Under Illinois Supreme Court precedent, Plaintiffs must allege that the conduct at issue occurred "primarily and substantially" in Illinois. *Avery v. State Farm Mut. Auto. Ins. Co.*, 216 Ill. 2d 100, 186, 835 N.E.2d 801, 854 (2005). Plaintiffs do not come close to satisfying this standard. Nor could they, because none of the relevant conduct occurred in Illinois. Relatedly, if BIPA applied to Clearview's conduct, then BIPA would violate the dormant Commerce Clause of the U.S. Constitution, which precludes the application of a state statute that has the effect of regulating conduct in another state.[1] Unlike Illinois, New York, where Clearview

[1] An Ill. Sup. Ct. R. 19 notice and the required documents will be served on the Illinois Attorney General.

is based, has no statutes regulating facial-recognition technology, despite having considered several. BIPA thus would be unconstitutional as applied because it would impose inconsistent obligations on Clearview and promote the public policy of Illinois over that of New York and other states.

Plaintiffs' claims also are barred by the First Amendment and Article One Section Four of the Illinois Constitution, which protect the creation and dissemination of information. As many cases have held, that protection includes the collection and use of public photographs that appear on the Internet. The First Amendment similarly protects Clearview's search engine that matches uploaded photos with publicly-available photos on the Internet. Plaintiffs' attempt to apply BIPA as a restriction on using "biometric information" impairs Clearview's First Amendment right to collect, analyze, and include public information in its search engine, and prevents the dissemination of that truthful and constitutionally-protected information. All challenged acts of Clearview relate to its use of what the Complaint refers to as "photographs of facial images from the internet," Compl. ¶ 1. In that context, Plaintiffs can neither survive the strict scrutiny applied in such cases or the requirement that regulations of expression be narrowly drawn so as to not limit free expression unduly.

Plaintiffs' BIPA claims in Counts Three and Four should be dismissed for another reason: Plaintiffs' allegations do not demonstrate that Clearview sold or in any way shared biometrics with a third-party and, as a result, Plaintiffs do not adequately allege a violation of BIPA Section 15(c), which provides that an entity may not "sell, lease, trade, or otherwise profit from" a person's biometrics. Plaintiffs' interpretation of Section 15(c)—as representing a blanket prohibition on profiting off of products involving biometrics—has never been accepted by any court, and is contrary to both the plain language of BIPA and its legislative history.

After dismissing the BIPA claims, the Court should next dismiss Counts Eight through Fourteen, which fail to state a claim under California, New York, or Virginia law. To begin with, Plaintiffs have not alleged an actual injury sufficient to establish standing under Article III for these claims. Counts Eight, Eleven, Twelve, and Fourteen—which attempt to allege right of publicity claims under state law—are each fatally flawed because Plaintiffs do not, and cannot, allege that Clearview used their likenesses for advertising or merchandising purposes, or to promote or sell goods or services. Count Thirteen should also be dismissed because Plaintiff Vestrand fails to allege a legally protected privacy interest, a reasonable expectation of privacy, or the type of "egregious" or "highly offensive" conduct that would satisfy the "high bar" required to state a claim under the California Constitution. Count Ten—a California Unfair Competition Law ("UCL") claim—also fails because it is derivative of Plaintiff Vestrand's other nonviable claims and because she alleges no loss of money or property, as required for standing under the UCL. And Count Nine should be dismissed because Plaintiff Roberson does not plead the basic elements of a Virginia Computer Crimes Act claim.

BACKGROUND

Clearview: Clearview is a small technology company headquartered in New York. Compl. ¶ 13. Clearview collects publicly-available images from the Internet, *id.*, and uses those images to create a searchable database, which allows authorized users (currently limited to governments or their agents or contractors) to identify unknown individuals by uploading a photograph, *id.* ¶ 1. Clearview's "algorithms compare[] the facial geometry of the subject appearing in a chosen photograph or video against the facial geometry of each of the hundreds of millions of subjects appearing in the database." *Id.* ¶ 32.

Individual Defendants: Ton-That is the CEO of Clearview, Schwartz is the President,

and Mulcaire is the General Counsel. *Id.* ¶¶ 14-16. Given that Clearview is a small start-up company, Schwartz has allegedly at times paid for certain Clearview costs, and Clearview allegedly directed its customers on occasion to send payments to Schwartz's residence. *Id.* ¶ 37. On one occasion, Mulcaire allegedly provided his personal information to the Illinois Secretary of State, resulting in the Illinois Secretary of State authorizing a payment to Mulcaire. *Id.* ¶ 41.

Rocky Mountain: Rocky Mountain is a special purpose entity that was used to contract with the Illinois Secretary of State. *Id.* ¶ 21. In or about September 2019, Rocky Mountain contracted with the Illinois Secretary of State to provide the Secretary of State with access to the Biometric Database. *Id.* ¶ 38. Other than the transaction with the Illinois Secretary of State, Rocky Mountain has not engaged in any other transactions related to Clearview's database. *Id.* ¶ 21.

ARGUMENT

I. The Complaint Fails to State a Claim Against the Individual Defendants and Rocky Mountain

As a threshold matter, Ton-That, Schwartz, and Mulcaire should be dismissed from this action because they cannot be held liable for actions they took while acting as officers and employees of Clearview.[2] "In diversity cases in which plaintiffs allege veil piercing claims, the Seventh Circuit has held that courts should apply the law of the state of incorporation." *Eagle Air Transp., Inc. v. Nat'l Aerotech Aviation Del., Inc.*, 75 F. Supp. 3d 883, 896 (N.D. Ill. 2014). Because Clearview is incorporated in Delaware, Compl. ¶ 13, Delaware law applies.

"Persuading a Delaware court to disregard the corporate entity is a difficult task." *Wallace v. Wood*, 752 A.2d 1175, 1183 (Del. Ch. 1999). "Effectively, the corporation must be a sham and

[2] Mulcaire and Rocky Mountain also should be dismissed because the Court lacks personal jurisdiction over them. For similar reasons previously discussed by Clearview, Mulcaire and Rocky Mountain did not purposefully avail themselves of Illinois to establish minimum contacts with the state. *See Mutnick v. Clearview AI, Inc.*, 20-cv-512, ECF No. 46 at 6-12, ECF No. 70 at 9-16.

exist for no other purpose than as a vehicle for fraud." *Id.* at 1184. Courts "*must* find an element of fraud to pierce the corporate veil." *Eagle Air Transp.*, 75 F. Supp. 3d at 896 (emphasis added).

Here, the Complaint does not contain a single allegation of fraud. Instead, Plaintiffs seek to pierce the corporate veil solely by alleging that Clearview was undercapitalized, Clearview's customers occasionally sent payments to Schwartz's residence, and Schwartz paid for some of Clearview's startup costs. Compl. ¶¶ 36-37. These allegations merely suggest that Clearview is a startup company. They come nowhere close to suggesting that Clearview "exist[s] *for no other purpose* than as a vehicle for fraud." *Wallace*, 752 A.2d at 1183 (emphasis added).

Similarly, Plaintiffs allege that there is no distinction between Clearview and Rocky Mountain based on allegations that Rocky Mountain is undercapitalized, at least one employee is shared between Clearview and Rocky Mountain, and a payment was supposedly made to Mulcaire instead of to Rocky Mountain. Compl. ¶¶ 40-41. Again, none of these allegations demonstrates fraud. Rocky Mountain's corporate purpose, as alleged in the Complaint, was to carry out a business transaction with the Illinois Secretary of State, which it is alleged to have done. *Id.* ¶ 21.

Moreover, all the claims against Rocky Mountain should be dismissed for another reason: Plaintiffs recite the statutory elements in a conclusory manner, rather than alleging any facts that demonstrate how those requirements have been satisfied. This is hardly surprising, given that Rocky Mountain is a special purpose vehicle and has no actual operations. For example, Count Two alleges that Rocky Mountain violated BIPA because "[i]n or about September 2019, Rocky Mountain collected, captured, purchased, received through trade and/or otherwise obtained the biometric identifiers and information of" Plaintiffs and class members. *Id.* ¶ 89.[3] Mere repetition

[3] Each of the other claims against Rocky Mountain is based on conclusory allegations that its activities "includ[e] collecting, obtaining, distributing, disseminating, selling, leasing and profiting from" biometrics. Compl. ¶ 42; *see id.* ¶ 104 (Count Four); ¶ 118 (Count Six); ¶ 125 (Count Seven); ¶ 134 (Count Eight);

of the statutory elements without factual support is insufficient to state a claim as a matter of law. *See Bissessur v. Ind. Univ. Bd. of Trs.*, 581 F.3d 599, 603 (7th Cir. 2009).

II. BIPA Does Not Regulate Out-Of-State Conduct

The Complaint should be dismissed as to all the Clearview Defendants because (1) BIPA does not apply to conduct outside of Illinois and (2) the application of BIPA to Clearview would violate the dormant Commerce Clause.

A. Plaintiffs' Claim Violates Illinois' Extraterritoriality Doctrine

Illinois has a "long-standing rule of construction" that a "statute is without extraterritorial effect unless a clear intent in this respect appears from the express provisions of the statute." *Avery*, 216 Ill. 2d at 184-85, 835 N.E.2d at 852. Because BIPA expresses no such intent, courts in Illinois have repeatedly held that BIPA does not regulate out-of-state conduct. *See, e.g.*, *Rivera v. Google, Inc.*, 238 F. Supp. 3d 1088, 1104 (N.D. Ill. 2017) ("[BIPA] was not intended to and does not have extraterritorial application."); *Monroy v. Shutterfly, Inc.*, No. 16 C 10984, 2017 WL 4099846, at *5 (N.D. Ill. Sept. 15, 2017) (same). The Illinois Supreme Court has explained that a "transaction may be said to take place within a state if the circumstances relating to the transaction occur[red] *primarily and substantially*" in Illinois. *Avery*, 216 Ill. 2d at 186, 835 N.E.2d at 854 (emphasis added). To satisfy this standard, the "*majority* of circumstances relating to the alleged violation" of the statute must have occurred in Illinois. *Landau v. CNA Fin. Corp*, 381 Ill. App. 3d 61, 65, 886 N.E.2d 405, 409 (1st Dist. 2008) (emphasis added). Accordingly, to state a BIPA claim, Plaintiffs must allege that the asserted violations primarily and substantially occurred in Illinois. *See Rivera*, 238 F. Supp. 3d at 1100. Illinois courts regularly grant motions to dismiss based on extraterritoriality where, as here, the complaint fails to allege that the relevant facts

¶ 156 (Count Ten); ¶ 164 (Count Eleven); ¶ 170 (Count Twelve); ¶ 177 (Count Thirteen); ¶ 187 (Count Fourteen); ¶ 193 (Count Fifteen); ¶ 201 (Count Sixteen).

occurred "primarily and substantially" in Illinois.[4]

Plaintiffs' BIPA claim fails because Plaintiffs do not, and cannot, allege that the "majority of circumstances" giving rise to the claim occurred in Illinois. The Complaint alleges that Clearview, Ton-That, and Schwartz "scraped three billion photographs of facial images from the internet" and "created a searchable biometric database," Compl. ¶ 1; that Clearview "markets its technology throughout the United States" and has business practices that "extend nationwide," *id.* ¶ 13; and that the Clearview Defendants "have sold unfettered access to the Biometric Database," ¶ 32. Plaintiffs do not allege that any of these activities took place in Illinois—let alone a "majority" of them. Nor can they, since they all occurred in New York, where Clearview is headquartered. *Id.* ¶ 13.

Nor do any alleged sales of Clearview's app in Illinois provide a sufficient nexus to Illinois to remedy the extraterritoriality problem. The Complaint fails to allege that Clearview's sales "primarily and substantially" occurred in Illinois, as would be required to state a claim under Illinois law. *See Rivera*, 238 F. Supp. 3d at 1100. In fact, only a small fraction of Clearview's app sales occurred in Illinois. As a result, Plaintiffs' BIPA claims should be dismissed.[5]

B. Applying BIPA to Clearview Would Violate the Dormant Commerce Clause

BIPA, as sought to be applied here, violates the dormant Commerce Clause of the U.S. Constitution. Under Article I, Section 8, Congress has the exclusive power to regulate commerce

[4] *See, e.g.*, *Vulcan Golf, LLC v. Google Inc.*, 552 F. Supp. 2d 752, 775 (N.D. Ill. 2008) ("While the plaintiffs contend that Illinois has 'significant contacts' with each of the named class plaintiffs because each is a resident of the state and each conducts substantial business in this state, the plaintiffs point to no allegations that plausibly suggest that the purported deceptive domain scheme occurred primarily and substantially in Illinois."); *Landau*, 381 Ill. App. 3d at 63-65, 886 N.E.2d at 407-09; *Phillips v. Bally Total Fitness Holding Corp.*, 372 Ill. App. 3d 53, 58-59, 865 N.E.2d 310, 315-16 (1st Dist. 2007).

[5] The residency of Plaintiffs and the putative class members does not change this conclusion. *See, e.g.*, *Avery*, 216 Ill. 2d at 182, 186 (explaining that the extraterritoriality analysis is not "based on the residency of the plaintiff").

"among the several States." This express grant of power limits the "authority of the States to enact legislation affecting interstate commerce." *Healy v. Beer Inst., Inc.*, 491 U.S. 324, 326 n.1 (1989). The "dormant Commerce Clause" "precludes the application of a state statute" that has "the practical effect of . . . control[ling] conduct beyond the boundaries of the State," "whether or not the commerce has effects within the State." *Id.* at 336. Absent this rule, "any state that has chosen a policy more *laissez faire* than [another state's] would have its choices stymied, because the state that has chosen more regulation could always trump its deregulated neighbor." *Morley-Murphy Co. v. Zenith Elecs. Corp.*, 142 F.3d 373, 379 (7th Cir. 1998). Illinois courts have taken a "broad[] view" of what constitutes an inconsistent legal regime for dormant Commerce Clause purposes. *Midwest Title Loans, Inc. v. Mills*, 593 F.3d 660, 667-68 (7th Cir. 2010). Specifically, a party need not show "inconsistent *obligations*"; rather, "the *absence* of a . . . counterpart" law in another state shows that the other state "thinks [the conduct] shouldn't be restricted in the [same] way." *Id.* at 667 (emphasis added).

Here, New York, among other states, has considered BIPA-style legislation multiple times in recent years, but has never enacted such legislation. *See* A1911, Assemb., Reg. Sess. (N.Y. 2019); S1203, Senate, Reg. Sess. (N.Y. 2019); A9793, Assemb., Reg. Sess. (N.Y. 2018); S8547, Senate, Reg. Sess. (N.Y. 2018). Because Illinois has no interest in regulating Clearview's alleged conduct in New York, and because New York has declined to adopt a statute regulating biometrics, the dormant Commerce Clause precludes application of BIPA to Clearview, as that would "exalt the public policy" of Illinois over that of New York. *Midwest Title Loans*, 593 F.3d at 668.[6]

[6] This principle is especially important in the Internet context. "[C]ourts have long recognized that certain types of commerce demand consistent treatment," and that the "Internet represents one of those areas." *Am. Libraries Ass'n v. Pataki*, 969 F. Supp. 160, 181 (S.D.N.Y. 1997); *see also Am. Booksellers Found. v. Dean*, 342 F.3d 96, 103 (2d Cir. 2003) ("Because the internet does not recognize geographic boundaries, it is difficult . . . for a state to regulate internet activities without project[ing] its legislation into other States.").

Applying BIPA to Clearview's conduct in New York would subject Clearview to liability under an Illinois statute because some small percentage of Clearview's alleged database of "three billion" publicly-available photographs contains images of Illinois residents. Compl. ¶ 29. Because often it is impossible to identify where a photo on the Internet comes from—or where the person in the photo resides—under Plaintiffs' application of BIPA, Clearview arguably could not collect *any* photographs on the public Internet simply because they *might* relate in some way to someone in Illinois. If Clearview attempted to collect photographs from the Internet—even those identified through metadata as having been taken outside of Illinois—under Plaintiffs' application of BIPA, Clearview would *still* risk liability under BIPA because an Illinois resident could appear in one of those photographs. This is not simply a problem for Clearview, but for other developers of facial recognition technology, who must use large data sets of facial images to train machine-learning algorithms. That precise risk is what renders BIPA, as applied here, unconstitutional. *See Midwest Title Loans*, 593 F.3d at 667-68.

III. Plaintiffs' Claim Is Barred by the First Amendment

Clearview assists government agencies—including law enforcement—in identifying perpetrators and victims of crimes. That has included identifying those who have engaged in sexual exploitation of children[7] and those who assaulted the Capitol on January 6, 2021.[8] Clearview does this by collecting publicly-available images from the Internet, analyzing them, and returning its search results to the law-enforcement entities that are licensed users of Clearview's

[7] Kashmir Hill & Gabriel J.X. Dance, *Clearview's Facial Recognition App Is Identifying Child Victims of Abuse*, N.Y. Times (Feb. 7, 2020), https://www.nytimes.com/2020/02/07/business/clearviewfacial-recognition-child-sexual-abuse.html.

[8] *See, e.g.*, Todd Shields, et al., *Selfie-Snapping Rioters Leave FBI a Trail of Over 140,000 Images*, Bloomberg (Jan. 16, 2021), https://www.bloomberg.com/news/articles/2021-01-16/selfie-snapping-rioters-leave-fbi-a-trail-of-over-140-000-images; Drew Harwell and Craig Timberg, *How America's Surveillance Networks Helped the FBI Catch the Capitol Mob*, Washington Post (April 2, 2021), https://www.washingtonpost.com/technology/2021/04/02/capitol-siege-arrests-technology-fbi-privacy/.

app. It compares those photos to ones provided it by its law-enforcement clients to determine if ones already publicly available on the Internet match ones submitted by law enforcement to Clearview's app.

All this is accomplished with Clearview's confidential search engine which uses machine-learning to compare photos of people whose images are publicly displayed on the Internet with those in the images provided to Clearview by law enforcement. That comparison involves Clearview, within its search engine, creating what are sometimes referred to as "facial vectors"—numerical hashes generated by a machine-learning algorithm which analyzes faces—and comparing them to the same sort of data from faces contained in the images provided by law enforcement. Such data are created within Clearview's search engine and are never made public or sold to anyone. They are simply a tool used within a search engine that allows Clearview to determine if there is a high degree of similarity between any public Internet image and those that law enforcement has provided.

Clearview's creation and use of its app is protected speech under the First Amendment. The U.S. Supreme Court has determined, in unambiguous language—repeated verbatim by the Illinois Supreme Court—that the "creation and dissemination of information are speech within the meaning of the First Amendment." *Sorrell v. IMS Health Inc.*, 564 U.S. 552, 570 (2011); *People v. Austin*, 2019 IL 123910, ¶ 31, 155 N.E.3d 439, 454. That is what Clearview does.

In *Sorrell*, the Supreme Court struck down, on First Amendment grounds, Vermont's Prescription Confidentiality Law, which provided that, absent a prescriber's consent, pharmacies and similar entities could not sell, disclose for marketing purposes, or use for marketing purposes "prescriber-identifying information." *Sorrell*, 564 U.S. at 558. In striking down the statute, the Court rejected the arguments that the Vermont law did not regulate speech, but rather just regulated

"access to information" or conduct. *Id.* at 568. "Facts, after all," held the Court, "are the beginning point for much of the speech that is most essential to advance human knowledge and to conduct human affairs. There is thus a strong argument that prescriber-identifying information is speech for First Amendment purposes." *Id.* at 570.

The same reasoning applies to BIPA's restrictions on using "biometric information," as well as Plaintiffs' other state and common-law claims. As applied to Clearview's conduct, Plaintiffs' interpretation of BIPA—as well as other state and common law restrictions on including "biometric information" in Clearview's database derived from publicly-available photographs—violates the First Amendment by inhibiting Clearview's ability to collect, analyze, and include the public information in its product, preventing dissemination of truthful information regarding the identity of individuals pictured in law-enforcement-submitted images.

As regards that aspect of Clearview's conduct, courts have repeatedly held that the activities of search engines constitute speech entitled to First Amendment protection because they require the types of judgments about what to publish that trigger free-speech protection. *See Search King, Inc. v. Google Tech., Inc.*, 2003 WL 21464568, at *4 (W.D. Okla. May 27, 2003). That Clearview's app uses computer code to help make these kinds of constitutionally-protected judgments does not change the analysis. *See, e.g., Junger v. Daley*, 209 F.3d 481 (6th Cir. 2000) ("Because computer source code is an expressive means for the exchange of information and ideas about computer programming, we hold that it is protected by the First Amendment").

Central to this case is the indisputable proposition that all information potentially relevant to this case is and has been publicly available. As the Complaint acknowledges, all challenged acts of Clearview relate to "photographs posted and accessible on the internet" on Facebook and other websites. Compl. ¶¶ 8-11. Although the dissemination of photographs portraying private

sexual conduct may well not be protected by the First Amendment, *Austin*, 2019 IL 123910, ¶ 119, 155 N.E.3d at 474, the republication of voluntarily-posted photographs on the Internet is. Once "truthful information [is] 'publicly revealed' or 'in the public domain,' a court may not constitutionally restrain its dissemination." *Smith v. Daily Mail Pub. Co.*, 443 U.S. 97, 103 (1979).

A Seventh Circuit case is illustrative of the proposition. In *Nieman v. VersusLaw, Inc.*, 512 F. App'x 635 (7th Cir. 2013), the plaintiff sued Yahoo!, Google, Microsoft, and VersusLaw, alleging that search engines operated by these companies enabled potential employers to find documents related to a lawsuit he had brought against a past employer, which allegedly caused the potential employers not to hire him due to his perceived litigiousness. *Id.* at 636. The Seventh Circuit affirmed dismissal on First Amendment grounds, holding that plaintiff's claims were barred because they were "based on the defendants' republication of documents contained in the public record, so they fall within and are barred by the First Amendment privilege." *Id*. at 638. A similar First Amendment privilege protects Clearview's publication of publicly-available photos published openly on the Internet.

Courts have thus repeatedly held that individuals have no right to privacy in materials they post on the Internet. *See United States v. Khan*, No. 15-cr-286, 2017 WL 2362572, at *8 (N.D. Ill. May 31, 2017) (holding that "[t]here is no expectation of privacy in a public Facebook page" because "[a]lthough a person generally has a reasonable expectation of privacy in the contents of his own personal computer . . . such an expectation may be extinguished 'when a computer user disseminates information to the public through a website'") (citations omitted), *aff'd*, 937 F.3d 1042 (7th Cir. 2019); *United States v. Adkinson*, 2017 WL 1318420, at *5 (S.D. Ind. Apr. 7, 2017) ("There is no expectation of privacy in an open Facebook page.") (citation omitted).[9]

[9] *See also Guest v. Leis*, 255 F.3d 325, 333 (6th Cir. 2001) ("Users [of the Internet] would logically lack a

A. BIPA Is a Content-Based and Speaker-Based Restriction Subject to Strict First Amendment Scrutiny and Presumptively Unconstitutional as Applied to Clearview

BIPA is a content-based statute because it "target[s] speech based on its communicative content." *Reed v. Town of Gilbert*, 576 U.S. 155, 163 (2015). Content-based regulations "are presumptively unconstitutional and may be justified only if the government proves that they are narrowly tailored to serve compelling state interests." *Nat'l Inst. of Family & Life Advocates v. Becerra*, 138 S. Ct. 2361, 2371 (2018) (citing *Reed*, 576 U.S. at 163) ("*NIFLA*"). In this case, BIPA attempts to burden speech that identifies individuals effectively through the use of certain technology; it is content-based because it attempts to burden such efforts to identify people merely *because* they are so effective (and therefore supposedly pose privacy concerns). But if the "biometric information" or "biometric identifiers" could not be used to identify the people, they would not be targeted by BIPA. In short, the statute targets attempts to identify people that it deems too dangerous (from a privacy standpoint) merely because of their effectiveness. That makes it content-based under *Reed* and *NIFLA*.

Plaintiffs have never even claimed that Clearview could be barred or limited from seeking to match photographs that appeared on Facebook or other websites with those uploaded by licensed users of Clearview's service if it were done in a particularly cumbersome way—hiring, for example, a vast team of researchers to review and match photos manually. Their objection is seeking to do functionally the same act by the use of modern technology. That makes the statute content-based and, under *Reed* and *NIFLA*, triggers strict scrutiny—scrutiny these Plaintiffs have

---

legitimate expectation of privacy in the materials intended for publication or public posting."); *Doe v. Yesner*, No. 3:19-cv-0136-HRH, 2019 WL 4196054 (D. Alaska Sept. 4, 2019) (holding that the use of photographs posted on plaintiff's social-media profile could not support claims for intrusion of solitude or public disclosure of private facts); *Nucci v. Target Corp.*, 162 So. 3d 146, 153 (Fla. Dist. Ct. App. 2015) ("We agree with those cases concluding that, generally, the photographs posted on a social networking site are neither privileged nor protected by any right of privacy, regardless of any privacy settings.").

never even argued that BIPA could survive.

BIPA is also a "speaker-based" restriction on speech that, under *Sorrell*, is subject to heightened First Amendment scrutiny. *Sorrell*, 564 U.S. at 569-570 ("Vermont's law imposes a content- and speaker-based burden on respondents' own speech. That consideration . . . requires heightened judicial scrutiny."). In *Sorrell*, the Supreme Court made clear that any law that imposes burdens on speech that apply to some speakers but not others, triggers heightened judicial scrutiny. *Id.* That is precisely what BIPA does in expressly exempting from its requirements "any financial institution or an affiliate of a financial institution that is subject to Title V of the federal Gramm-Leach-Bliley Act of 1999" and any "contractor, subcontractor, or agent of a State agency or local unit of government when working for that State agency or local unit of government." 740 ILCS 14/25(c), (e). Given that these exceptions treat different speakers differently, *Sorrell* mandates that the court subject them to heightened judicial scrutiny. *Sorrell*, 564 U.S. at 570-71. Remarkably, Plaintiffs have argued that "BIPA's text makes clear that the exemption only includes conduct undertaken when working for Illinois agencies or local units of government in Illinois" and not that of the Federal or any other state government. Pls.' Reply in Supp. of Mot. for Expedited Discovery, Dkt. 46. As we point out elsewhere, that is in flat violation of the dormant Commerce Clause of the Constitution. But it is also proof of a First Amendment violation. BIPA prioritizes the speech of agents of Illinois government units and agencies over that of non-Illinois government units. A more speaker-based restriction is hard to imagine.

The Court in *Sorrell* referred back to its earlier ruling in *United States v. O'Brien*, 391 U.S. 367, 384 (1968), and stated that "the inevitable effect of a statute on its face may render it unconstitutional." *Sorrell*, 564 U.S. at 565. Here, BIPA's inevitable effect would be nothing less than preventing the identification of individuals whose published photographs were on the Internet.

The First Amendment simply does not permit a state to accomplish this goal. BIPA takes issue with the efficiency of Clearview's app—made possible by the use of facial vectors—that allegedly triggers the privacy concerns that BIPA is designed to protect. But the First Amendment prohibits the application of laws that have the purpose and/or practical effect of burdening speech by reducing the effectiveness of its content. *See Sorrell*, 564 U.S. at 565 (striking down law as content-based, in part, because its "purpose and practical effect are to diminish the effectiveness of marketing by manufacturers of brand-name drugs").

B. As Applied to Clearview, BIPA Is Subject to and Cannot Survive Strict Scrutiny

Because BIPA imposes content-based restrictions on Clearview's speech, it is subject to strict scrutiny. That demanding standard cannot be met unless "the restriction furthers a compelling interest and is narrowly tailored to achieve that interest." *Reed*, 576 U.S. at 171 (2015) (internal quotation marks and citation omitted). Understandably enough, Plaintiffs have made no such claim.

BIPA serves no compelling state interest with respect to already-published public information. The stated purpose of BIPA is to protect the privacy of Illinois citizens. *See, e.g.*, *Bryant v. Compass Grp. USA, Inc.*, 958 F.3d 617, 619 (7th Cir. 2020) (finding that BIPA's "regime is designed to protect consumers against the threat of irreparable privacy harms"). Specifically, BIPA purports to protect material that is "confidential and sensitive." 740 ILCS 14/15(e)(2). But as in this case, any information that an individual makes available to the general public is by definition not "confidential" or "sensitive." An individual's right to control their biometric information under BIPA does not apply if that right is relinquished. *See United States v. Caira*, 833 F.3d 803, 806 (7th Cir. 2016) (recognizing no expectation of privacy in information already disclosed to third-parties); *Rodriguez-Ruiz v. Microsoft Operations Puerto Rico, L.L.C.*, 2020 WL

1675708, at *3 (D. P.R. Mar. 5, 2020) ("Various courts have held that '[i]nformation posted on a private individual's social media "is generally not privileged, nor is it protected by common law or civil law notions of privacy."'") (citations omitted).

The Supreme Court "consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." *Smith v. Maryland*, 442 U.S. 735, 743-44 (1979); *accord Caira*, 833 F.3d at 806; *see also* Restatement (Second) of Torts § 652D (1977) ("[T]here is no liability for giving further publicity to what the plaintiff himself leaves open to the public eye."). This is particularly well established with respect to photographs posted on the Internet. *See United States v. Emmett*, 321 F.3d 669, 672 (7th Cir. 2003) ("[W]e think it clear that a person has no expectation of privacy in a photograph of his face.").

Even if the state had a compelling interest in protecting the privacy of individuals who placed photographs of themselves in the public realm (and it does not), BIPA is not narrowly tailored to achieve that interest. As applied to Clearview, BIPA would require Clearview to provide written notice to the individuals whose photographs are in Clearview's database and obtain a "written release" before collecting their "biometric information." 740 ILCS 14/15(b). But the individuals who posted their photographs on the Internet effectively consented to sharing their "biometric information," which is embedded in their photographs, with the public at large. *See, e.g.*, *Caira*, 833 F.3d at 806 ("[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties[.]").

C. BIPA Is Unconstitutionally Overbroad and Thus Cannot Withstand Intermediate Scrutiny as Applied to Clearview

Even if strict scrutiny were not applied in this case, the statute would be unconstitutionally overbroad and thus could not withstand even intermediate scrutiny. A statute "lacks the precision that the First Amendment requires when a statute . . . effectively suppresses a large amount of

speech that adults have a constitutional right to receive and to address to one another." *Reno v. ACLU*, 521 U.S. 844, 874 (1997); *accord Austin*, 2019 IL 123910, ¶ 89, 155 N.E.3d at 466-6 (a First Amendment challenge based on "overbreadth is permitted out of concern that the threat of enforcement of an overbroad law may chill or deter constitutionally protected speech").

Here, because of the limited ability to discern where subjects of online photographs may reside, BIPA all but bars—and certainly severely burdens—Clearview's right to use previously-published, publicly-displayed photographs in a manner that enables Clearview to match them with other photographs. In doing so, BIPA "suppresses a large amount of speech" that is fully protected under the First Amendment, precisely what the overbreadth doctrine exists to protect against. *Reno*, 521 U.S. at 874.

BIPA, as interpreted by Plaintiffs, is not narrowly drafted. It would require Clearview to purge from its database facial vectors of individuals whose residencies are unknown to it and who have already consented to the general public viewing their photos. The effect of this overly-broad drafting would be to require Clearview to abandon its constitutionally-protected business activities. Such a requirement cannot withstand constitutional muster.

IV. The Complaint Does Not Adequately Allege A Violation of Section 15(c)

Plaintiffs' allegations cannot support a violation of BIPA Section 15(c), which prohibits a private entity from selling, leasing, trading, or otherwise profiting from biometrics. Plaintiffs' allegations of a violation of Section 15(c) are based on the conclusory allegations that Clearview "sold unfettered access to the Biometric Database." Compl. ¶ 32. However, none of their factual allegations describe Clearview's customers receiving access to a biometric database. Rather, they have alleged that Clearview's users have the ability to "query" a database, which causes an algorithm to analyze the facial vectors of subjects in the database in order to identify an individual. *Id.* To be clear, Plaintiffs do not allege that the customers who query Clearview's database ever

receive access to biometrics. Thus, any allegation that Clearview has sold, leased, or traded biometrics is conclusory and should be rejected. *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009).

That leaves only the allegation that Clearview "profited from" biometrics in violation of Section 15(c) because it profited from technology that relies on biometrics. Compl. ¶ 54. This reading of BIPA should be rejected as contrary to the express purpose of BIPA. Section 15(c) does not prohibit a company from profiting from technology that utilizes biometric data. Indeed, the very purpose of BIPA is to "regulat[e]"—not eliminate—"biometric-facilitated transactions." 740 ILCS 14/5(c), (g).

Section 15(c) is clear on its face. An entity may not transfer a person's biometric data to another in exchange for any consideration. 740 ILCS 14/15(c). That is the plain meaning of each of the three verbs—"sell, lease, trade"—that are specifically enumerated in § 15(c).[10] The General Assembly's addition of the ancillary phrase "sell, lease, trade, *or otherwise profit from* [biometric data]," 740 ILCS 14/15(c) (emphasis added), must be interpreted using "the cardinal rule of statutory construction known as *ejusdem generis*," which provides that, "when a statutory clause specifically describes several classes of persons or things and then includes 'other persons or things,' the word 'other' is interpreted to mean 'other such like.'" *Pooh-Bah Enters., Inc. v. Cty. of Cook*, 232 Ill. 2d 463, 492, 905 N.E.2d 781, 799 (2009). The clause "or otherwise profit from" is therefore meant to reinforce the prohibition on transferring biometric data for profit; it is not meant to prohibit completely separate acts related to the mere possession of biometrics. *See Dean v. Smith*, 2017 IL App (1st) 170404, ¶ 25, 84 N.E.3d 379, 385; *see also Pooh-Bah Enters.*, 232 Ill.

[10] *See Black's Law Dictionary* 1567 (10th ed. 2014) (defining "sell" as "[t]o transfer (property) by sale"); *id.* at 1026 (defining "lease" as "[t]o grant the possession and use of (land, buildings, rooms, movable property, etc.) to another in return for rent or other consideration"); *id.* at 1720-21 (defining "trade" as "[a] transaction or swap").

2d at 492, 905 N.E.2d at 799.

That Section 15(c) was not meant as a prohibition on biometric transactions is clear from BIPA's legislative history. When BIPA was being considered by the Illinois House, Representative Kathleen A. Ryg, a sponsor of BIPA, explained that the origin of the statute was the bankruptcy of Pay By Touch, and the concern that consumers' biometric data could be sold in a bankruptcy court auction. 95th Ill. Gen. Assemb., House Proceedings, May 30, 2008, at 249. Thus, there was a "very serious need of protections for . . . biometric information"—specifically, "prohibiting the sale of biometric information." *Id.*; *see also Sekura v. Krishna Schaumburg Tan, Inc.*, 2018 IL App (1st) 180175, ¶ 64, 115 N.E.3d 1080, 1094 ("Representative Ryg's remarks establish [] the primary impetus behind the bill."). Representative Ryg's concerns over the possible sale of Pay By Touch's database in bankruptcy show that the legislature sought to prohibit the sale of biometric data—not the business of using biometric technology.

Indeed, if Section 15(c) were construed to prohibit *any* profitmaking activity related to biometric technology, BIPA's entire statutory framework would become unnecessary. All commercial use of biometric data in Illinois would grind to a halt, and the very purpose of BIPA—to "regulat[e]" "biometric-facilitated transactions"—would be eliminated. 740 ILCS 14/5(c), (g). The legislature, however, made clear that it passed BIPA to encourage the "use of biometrics." 740 ILCS 14/5(a) (setting forth BIPA's "Legislative Findings [and] Intent"). The legislature's intent in "[p]utting these regulations in place" was to "further the selection by '[m]ajor national corporations' of 'the City of Chicago and other locations in this State as pilot testing sites for new applications of biometric-facilitated financial transactions. . . .'" *Sekura*, 2018 IL App (1st) 180175, ¶ 58, 115 N.E.3d at 1093 (quoting 740 ILCS 14/5(b)). Plaintiffs' reading of Section 15(c)—that it was a prohibition on for-profit technologies that involve biometrics—directly

conflicts with this express legislative intent and should be rejected.

V. BIPA Does Not Apply to Clearview's Use of Photographs

As yet another basis for dismissing the BIPA claims, the plain language of BIPA expressly excludes both photographs and information derived from photographs from its reach, and so BIPA does not apply to Clearview's product. BIPA covers two categories of information: (1) original sources of information about a person ("biometric identifiers," defined as a "retina or iris scan, fingerprint, voiceprint, or scan of hand or face geometry") and (2) data derived from those sources ("biometric information," defined as "information . . . based on an individual's biometric identifier"). 740 ILCS 14/10. BIPA's definition of "biometric identifiers" excludes "photographs," and its definition of "biometric information" excludes "information derived from items or procedures excluded under the definition of biometric identifiers," such as photographs. *Id.* Accordingly, the legislature excluded both photographs and information derived from photographs from BIPA's reach. Because Clearview's product is based only on photographs and information derived therefrom, Clearview's product is outside the scope of BIPA.

VI. Plaintiffs Fail to State a Claim Under California, New York, or Virginia Law

Plaintiffs also bring a litany of "kitchen sink" claims under California, New York, and Virginia law (Counts Eight through Fourteen). All of these claims should be dismissed.

A. Plaintiffs Fail to Allege a Cognizable Injury to Support Article III Standing

As a threshold matter, Counts Eight through Fourteen should be dismissed because Plaintiffs fail to allege a cognizable Article III injury. To survive a motion to dismiss, allegations of actual injury must be both plausible and causally linked to the conduct complained of. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560-61 (1992). It is not enough to invoke a vague and nebulous right to "privacy"; the alleged injury must be "concrete" and "actually exist" and cannot be "abstract." *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016). The allegations here

demonstrate that Plaintiffs' privacy interests have not been injured (because the information at issue does not implicate a protected privacy interest under California, New York, or Virginia law), and the alleged dissemination of their information did not result in any concrete harm (because Plaintiffs fail to allege that they lost money or suffered a serious threat of identity theft).

The mere fact of sharing information does not give rise to a cognizable privacy injury. A "party that has brought statutory or common law claims based on nothing more than the unauthorized disclosure of personal information" has no "standing" on that basis alone. *In re Google, Inc. Privacy Policy Litig.*, No. C 12-01382, 2012 WL 6738343, at *5 (N.D. Cal. Dec. 28, 2012). Instead, courts consider the nature of the information that was shared, and if it does not pose a significant risk of real-world harm, or if the party obtaining the information did not intend to commit identity theft or cause other injury using the data, there is no standing. *See Antman v. Uber Techs., Inc.*, 3:15-cv-1175, 2015 WL 6123054, at *11 (N.D. Cal. Oct. 19, 2015).

Plaintiffs' theories of injuries and damages are entirely based on their allegations that Clearview "captured" and "disseminated" their biometric information, thereby "exposing them to the imminent and certainly impending injuries of identity theft, fraud, stalking, surveillance, social engineering and other invasions of privacy." Compl. ¶¶ 60-61. But Plaintiffs do not allege that they (or any putative class members) were the victims of identity theft due to Clearview's conduct; nor do they plead facts explaining how Clearview created an "imminent and certainly impending" injury to them.[11] *Id.* ¶ 61. The only use of Plaintiffs' information identified in the Complaint is in a "Biometric Database" that was made accessible to certain "law enforcement agencies" and

[11] Among other things, Plaintiffs assert that Clearview has "lax security practices" based on unsupported allegations that hackers obtained Clearview's "customer list" and a "misconfigured server." Compl. ¶¶ 33-34. These allegations are irrelevant. These "hacks" did not impact any facial vectors, and Plaintiffs do not—and cannot—identify any Clearview data breach that exposed their facial vectors or caused them injury in any way.

"private companies"—but those allegations do not explain how Plaintiffs' information, derived from publicly-available photographs, could be used for identity theft or any other actionable invasions of privacy. *Id*. ¶¶ 31-32.

Moreover, a claim based on a *bona fide* risk of identity theft exists only where the information, if stolen, is likely to cause imminent economic harm by facilitating access to financial data or accounts. But here, Plaintiffs fail to allege that Clearview released information such as "social security numbers," *Krottner v. Starbucks Corp.*, 628 F.3d 1139, 1140 (9th Cir. 2010), that gives an identity thief "all the information he need[s] to open accounts or spend money in the plaintiffs' names," *In re Zappos.com, Inc.*, 888 F.3d 1020, 1026 (9th Cir. 2018).[12] Accordingly, Counts Eight through Fourteen should be dismissed because Plaintiffs fail to articulate a cognizable injury.

B. Plaintiffs Fail to State a Claim under State "Right of Publicity" Laws

In Counts Eight, Eleven, Twelve, and Fourteen of the Complaint, Plaintiffs purport to allege violations of California, New York, and Virginia state law governing the right of publicity, which protect against the misappropriation of one's likeness in merchandising or advertising—that is, it protects an individual's *economic interest* in his or her likeness. *See Maloney v. T3Media, Inc.*, 853 F.3d 1004, 1010 (9th Cir. 2017). These state laws are simply inapplicable here.

To begin, Plaintiffs selectively quote from statutory text to disguise the fact that the right of publicity governs the unauthorized use of a person's photograph or likeness only in *advertising* or *merchandising*. The Complaint states that the California statute "makes it unlawful for any

[12] *See, e.g.*, *Beck v. McDonald*, 848 F.3d 262, 267-68 (4th Cir. 2017) (risk of identity theft following hospital data breach that disclosed patients' "names, birth dates, the last four digits of social security numbers, and physical descriptors (age, race, gender, height, and weight)" was "too speculative to confer standing"); *Antman*, 2015 WL 6123054, at *11 ("theft of names and driver's licenses" was insufficient to create standing where the complaint failed to adequately allege an "obvious, credible risk of identity theft that risks real, immediate injury").

person to knowingly 'use another's . . . photograph [] or likeness, in any manner . . . without such person's prior consent. . . .'" Compl. ¶ 162 (alterations in original) (quoting Cal. Civ. Code § 3344(a)). But Plaintiffs omit the specific statutory language that sinks their claim: § 3344(a) applies where a person "knowingly uses another's . . . photograph[] or likeness, in any manner, *on or in products, merchandise, or goods, or for purposes of advertising or selling, or soliciting purchases*. . . ." Cal. Civ. Code § 3344(a) (emphasis added); *see also Maloney*, 853 F.3d at 1004.

Despite the clear scope and purpose of § 3344(a), nowhere does the Complaint attempt to plausibly allege that Clearview used Plaintiff Vestrand's photographs or likeness in advertising or merchandising. Plaintiff Vestrand merely alleges that her information is a part of database that some clients pay to access—and according to Plaintiffs' theory, Clearview has gathered this information from publicly-available photographs for further "disseminat[ion]" to the public, not for use in advertising or merchandising. Compl. ¶¶ 48-50, 60.[13]

Plaintiff Vestrand thus fails to state a claim in Count Eleven for the simple reason that § 3344(a) has nothing to do with Clearview's conduct or business model as alleged in Complaint. *See Callahan v. Ancestry.com Inc.*, 20-cv-08437, 2021 WL 783524, at *5 (N.D. Cal. Mar. 1, 2021) (dismissing § 3344(a) claim because "Ancestry's use of the plaintiffs' profiles does not imply an endorsement of Ancestry's products"). This analysis also applies to California's common law right of publicity, and Count Twelve fails for the same reasons as Count Eleven. *See Maloney*, 229 Cal. App. 4th at 1011 & n.16.

The same is true of Plaintiffs' other right of publicity claims under New York and Virginia

[13] If Plaintiff Vestrand's reading of the right of publicity statutes were correct, it would yield absurd results: every individual whose photograph has ever appeared in an Internet search would have a right of publicity claim against the search engines that linked to those photographs in their search results. The result would be the end of the Internet as we have come to know it. That is not, and cannot be, the law.

law. The New York and Virginia statutes apply where a person's "portrait" or "picture" is used, without consent, "for advertising purposes or for the purposes of trade." N.Y. Civ. Rights Law § 51; Va. Code § 8.01-40. Again, Plaintiffs allege no facts showing that Clearview used Plaintiffs' photographs for advertising purposes. Instead, Plaintiffs lean on the more ambiguous term "for the purposes of trade," which is not defined in either state's statute. Compl. ¶¶ 134, 187. However, courts applying New York and Virginia law have explained that a "trade purpose" exists only where an individual's name or likeness is used to promote or sell goods or services, which is not alleged to have occurred here.[14] Thus, Counts Eight and Fourteen should also be dismissed.[15]

Further, Plaintiffs also fail to state a publicity-right claim for the independent reason that Clearview's use of Plaintiffs' photographs has a protected public interest purpose. As discussed in Part III, *supra*, any right of publicity must yield to constitutional free-speech interests when the two are in conflict. Accordingly, publicity-right laws have "been narrowly construed by the courts" to avoid conflict with the First Amendment. *Ann-Margret v. High Soc. Mag., Inc.*, 498 F. Supp. 401, 404 (S.D.N.Y. 1980). Indeed, California, New York, and Virginia law exempts liability for the use of individuals' photographs and likenesses in a public-affairs context. *See* Cal. Civ. Code § 3344(d); *Williams v. Newsweek, Inc.*, 63 F. Supp. 2d 734, 736 (E.D. Va.), *aff'd*, 202 F.3d

---

[14] *See Motise v. Am. Online, Inc.*, Civ.A. 04-1494, 2005 WL 1667658, at *3 (E.D. Va. June 24, 2005) ("Plaintiff must allege that Defendant used his name specifically for the purpose of advertising or solicitation for patronage of a product, and Plaintiff must provide some facts that support such a theory."); *Otero v. Houston Street Owners Corp*, No. 104819/2010, 2012 WL 692037, at *2 (N.Y. Sup. Ct. Feb. 28, 2012) (dismissing §§ 50-51 claim based on use of surveillance camera for failure to allege a trade purpose, explaining that a "picture is used for trade purposes if its use is to attract trade to a business entity.").

[15] Plaintiffs attempt to circumvent the straightforward pleading requirements for a right of publicity claim by alleging that Clearview "disclosed" and "disseminated" plaintiffs' information "for commercial gain." Compl. ¶¶ 60, 164, 170. But this conduct is not actionable as a publicity-right claim. Sharing "information with third parties is categorically different from the type of conduct made unlawful by this tort, such as using a plaintiff's face or name to promote a product or service." *In re Facebook, Inc., Consumer Priv. User Profile Litig.*, 402 F. Supp. 3d 767, 803 (N.D. Cal. 2019); *see also Ancestry.com*, 2021 WL 783524, at *5 ("the plaintiffs do not have a commercial interest in their public profiles that precludes Ancestry's use of the profiles for commercial gain").

262 (4th Cir. 1999); *Ann-Margret*, 498 F. Supp. at 404. Plaintiffs allege, in conclusory fashion, that Clearview's use of their photographs "did not have any connection with . . . public affairs." Compl. ¶ 165. But courts have explained that the "public affairs" exception focuses on the "purpose" in using a person's information; where, as here, the "purpose is informative . . . the use is immune." *New Kids On The Block v. News Am. Pub., Inc.*, 745 F. Supp. 1540, 1546 (C.D. Cal. 1990), *aff'd*, 971 F.2d 302 (9th Cir. 1992) ("gathering information for dissemination to the public" is protected speech) (internal quotation marks omitted).[16] According to the Complaint, Clearview's purpose was to gather information for dissemination to the public—an activity protected by the First Amendment. As a result, these claims should be dismissed.

C. Plaintiff Vestrand Fails to State a Privacy Claim under the California Constitution

"The California Constitution sets a 'high bar' for establishing an invasion of privacy claim." *In re Yahoo Mail Litig.*, 7 F. Supp. 3d 1016, 1038 (N.D. Cal. 2014) (citation omitted). To clear this bar, a plaintiff must plead (1) a legally protected privacy interest; (2) a reasonable expectation of privacy in the circumstances; and (3) a serious invasion of privacy constituting "an egregious breach of . . . social norms." *Hill v. Nat'l Collegiate Athletic Ass'n*, 7 Cal. 4th 1, 35–37 (1994). But here, Plaintiff Vestrand fails to plead any of these three elements.

First, Plaintiff Vestrand fails to allege a legally protected privacy interest. Plaintiff Vestrand states neither an informational interest—which pertains to "the dissemination or misuse of sensitive and confidential information" that, if disclosed, could cause "unjustified embarrassment or indignity"; nor an autonomy interest—which shields "intimate personal

[16] The mere fact that Clearview's use of Plaintiffs' photographs may have been "spurred by the profit motive and engaged in the commercial exploitation does not negate [its] right to depict matter of public interest." *Newsweek*, 63 F. Supp. 2d at 736 (citation and alterations omitted).

decisions" from "observation" or "intrusion." *Pioneer Elecs. (USA), Inc. v. Superior Ct.*, 40 Cal. 4th 360, 370 (2007). Plaintiff Vestrand does not allege that Clearview collected and misused extremely personal and sensitive information—Clearview did not, for example, disclose anyone's mental health records, HIV-positive status, or sexual history. *C.f. Botello v. Morgan Hill Unified Sch. Dist.*, No. C09-02121 HRL, 2009 WL 3918930, at *5 (N.D. Cal. Nov. 18, 2009) (sexual history); *Susan S. v. Israels*, 55 Cal. App. 4th 1290, 1294 (1997) (mental health records); *Urbaniak v. Newton*, 226 Cal. App. 3d 1128, 1133 (1991) (HIV-positive status).

Second, Plaintiff Vestrand fails to plead that she had a reasonable expectation of privacy over her publicly-posted photographs. To prevail on this claim, "the plaintiff must have conducted himself or herself in a manner consistent with an actual expectation of privacy." *Moreno v. Hanford Sentinel, Inc.*, 172 Cal. App. 4th 1125, 1129 (2009); *see also Yahoo Mail*, 7 F. Supp. 3d at 1037-38. In *Moreno*, the court dismissed the plaintiff's constitutional privacy claim, which was based on allegations that a newspaper invaded the plaintiff's privacy by disseminating content posted on her Myspace page. The court concluded that "no reasonable person would have had an expectation of privacy" under the circumstances, after the plaintiff's "affirmative act" of posting the content online made it "available to any person with a computer and thus opened it to the public eye." *Id*. at 1130. Likewise, Plaintiff Vestrand had no reasonable expectation of privacy over content she chose to upload to public websites on the Internet. Compl. ¶ 50.

Third, Plaintiff Vestrand cannot establish an egregious breach of social norms because courts routinely refuse to characterize the collection or dissemination of personally identifying information as "egregious" violations.[17] The claim here is even weaker because Plaintiff Vestrand

[17] *See, e.g.*, *Stern v. Weinstein*, No. 09-CV-1986, 2010 WL 11459791, at *6 (C.D. Cal. Jan. 6, 2010), *aff'd*, 512 F. App'x 701 (9th Cir. 2013) (the complaint did "not present a 'sufficiently serious' invasion of privacy" where "Plaintiff voluntarily shared his posting with approximately 2,300 [] listserv members" and

herself voluntarily disclosed her information. *Id.*

D. Plaintiff Vestrand's Derivative and Unviable Unfair Competition Law Claim Should Be Dismissed

Count Ten attempts to state a claim under California's Unfair Competition Law ("UCL"). To have standing under California law to pursue this claim (a standard that is different from Article III standing), Plaintiff Vestrand must show that she "lost money or property" because of Clearview's conduct. *Huynh v. Quora, Inc.*, No. 18-CV-07597-BLF, 2019 WL 11502875, at *6 (N.D. Cal. Dec. 19, 2019); *see also* Cal. Bus. & Prof. Code § 17204. Plaintiff Vestrand lacks standing to bring this claim because she did not pay money to Clearview, or lose money or property due to Clearview's conduct.[18] Clearview "may have gained money through its sharing or use of the Plaintiffs' information" but "that's different from saying the plaintiffs lost money." *Id.* at *7 (citation omitted). Accordingly, the UCL claim fails at the outset for lack of standing.

Plaintiff Vestrand also cannot plausibly allege that Clearview's conduct was either "unfair" or "unlawful." First, claims of "unfair" conduct are available only in the context of *competition* claims, which Plaintiff Vestrand has not alleged here. *See Durell v. Sharp Healthcare*, 183 Cal. App. 4th 1350, 1366 (2010). And second, Clearview's conduct was not unlawful: Plaintiff Vestrand's UCL claim is derivative of a series of claims that—as explained in Parts VI.B-C, *supra*—Plaintiff Vestrand fails to adequately allege.[19] The only non-derivative allegation is her

"[a]bsent any allegation of the unauthorized accessing or disclosure of sensitive medical information or comparably sensitive or embarrassing information, this claim fails."); *In re Google, Inc. Privacy Policy Litig.*, 58 F. Supp. 3d 968, 987–88 (N.D. Cal. 2014) (disclosure of names, identities, contact lists, private user information, and contents of communications to third-parties was not highly offensive).

[18] Personal information is not property for purposes of standing under the UCL. *See In re Facebook Priv. Litig.*, 791 F. Supp. 2d 705, 714 (N.D. Cal. 2011), *aff'd*, 572 F. App'x 494 (9th Cir. 2014) ("personal information does not constitute property for purposes of a UCL claim").

[19] Plaintiff Vestrand also claims that Clearview violated the UCL by "[f]ailing to provide adequate data security of the data they have collected." Compl. ¶ 151. This allegation is not actionable under the UCL, which only permits "unlawful" claims if they are premised on statutory, regulatory, or court-made law. The Complaint does not tie this "data security" allegation to any such law, and accordingly, it provides no basis

claim that Clearview violated the UCL by "[f]ailing to comply with § 1798.100(b) of the California Consumer Privacy Act ('CCPA')." Compl. ¶ 151 (citing Cal. Civ. Code § 1798.100 *et seq.*). But this claim also fails, because the CCPA "only" confers a private right of action for violations of subsection (a) of § 1798.150, which pertains to data breaches, and expressly precludes a cause of action "based on violations of any other section" of the CCPA. *See* Cal. Civ. Code § 1798.150(a), (c). It also prohibits a plaintiff from using the CCPA "to serve as the basis for a private right of action *under any other law*." *Id.* § 1798.150(c) (emphasis added). Here, Plaintiff Vestrand does not allege that her information was subject to a data breach within the meaning of § 1798.150(a)—instead, she bases her UCL claim on a different CCPA provision, subsection (b) of § 1798.100. Compl. ¶ 151. But there is simply no private right of action for a violation of § 1798.100(b), and Plaintiffs' UCL claim predicated on the CCPA therefore fails as a matter of law.

E. The Complaint Does Not Adequately Allege a Violation of the Virginia Computer Crimes Act

Count Nine should be dismissed because Plaintiff Roberson fails to allege any specific violations of the Virginia Computer Crimes Act ("VCCA"), Va. Code § 18.2–152.1 *et seq.* The VCCA is a *criminal* anti-hacking statute intended to target malicious computer break-ins—it was never intended to police access to publicly available information on the Internet.[20] Plaintiff Roberson's claim fails on multiple fronts.

---

for an "unlawful" claim. *See Shroyer v. New Cingular Wireless Servs., Inc.*, 622 F.3d 1035, 1044 (9th Cir. 2010) ("[Plaintiff] must also allege that [defendant] engaged in a business practice 'forbidden by law, be it . . . statutory, regulatory, or court-made.' . . . Because [Plaintiff] does not go beyond alleging a violation of common law, he fails to state a claim under the unlawful prong of § 17200.").

[20] "The elements of a violation of [Va. Code § 18.2–152.3] are that the defendant (1) uses a computer or computer network; (2) without authority; and (3) either obtains property or services by false pretenses, embezzles or commits larceny, or converts the property of another." *Cvent, Inc. v. Eventbrite, Inc.*, 739 F. Supp. 2d 927, 934 (E.D. Va. 2010) (citing Va. Code § 18.2–152.3). Other provisions of the VCCA cited in the Complaint similarly require a showing that the defendant used a computer or computer network "without authority." *See* Va. Code §§ 18.2–152.4, 18.2–152.5.

As an initial matter, for the reasons discussed in Part VI.A, *supra*, Plaintiff Roberson fails to plead an actual injury or legally cognizable damages, which are requirements to state a claim under the VCCA. *See* Va. Code § 18.2–152.12(A).

Second, Plaintiff Roberson fails to allege that Clearview used any computer or computer network "*without authority*." "It is the unauthorized use of a computer network that gives rise to liability under the VCCA." *In re Hackman*, 534 B.R. 867, 879-80 (Bankr. E.D. Va. 2015).

Third, Plaintiff Roberson fails to allege false pretenses, conversion, artifice, trickery, or deception. Instead, while the Complaint points to allegedly "unlawful 'scraping' techniques . . . [a]t no point does the complaint plead specific facts giving rise to a plausible inference of larceny, false pretenses, embezzlement, or conversion, as required by the plain text of the VCCA." *Cvent*, 739 F. Supp. 2d at 935. "Scraping" is not "larceny, false pretenses, embezzlement, or conversion" nor is it "artifice, trickery or deception." [21] *Id.*; Va. Code § 18.2–152.5:1. As a result, Plaintiff Roberson fails to state a claim.

VII. Plaintiffs Fail to State a Claim for Unjust Enrichment

Plaintiffs' unjust enrichment claim is not viable under the laws of California, New York, Virginia, or Illinois, and as a result, Count Fifteen should be dismissed.

California: "[T]here is no cause of action for unjust enrichment under California law." *Low v. LinkedIn Corp.*, 900 F. Supp. 2d 1010, 1031 (N.D. Cal. 2012) (collecting cases).[22]

[21] To the contrary, courts have recognized that automated scraping of publicly accessible data likely does not violate the substantively similar Computer Fraud and Abuse Act, 18 U.S.C. § 1030. *See hiQ Labs, Inc. v. LinkedIn Corp.*, 938 F.3d 985, 999-1000 (9th Cir. 2019) (affirming a preliminary injunction to prevent LinkedIn from blocking hiQ Labs from "scraping" information in publicly available LinkedIn profiles).

[22] The unjust enrichment claim also fails because Plaintiff Vestrand must show that Clearview—by engaging in an "actionable wrong"—obtained a specific benefit at her expense. *Rojas-Lozano v. Google, Inc.*, 159 F. Supp. 3d 1101, 1120 (N.D. Cal. 2016). Here, Plaintiff Vestrand fails to allege any actionable wrong. *Swearingen v. Healthy Beverage, LLC*, No. 13-CV-04385, 2017 WL 1650552, at *5 (N.D. Cal. May 2, 2017) (dismissing unjust enrichment claim for same reasons as the UCL and CLRA claims).

New York: Under New York law, "[c]ommon-law unjust enrichment claims for the unauthorized use of an image or likeness are preempted by Civil Rights Law §§ 50 and 51." *Sondik v. Kimmel*, 131 A.D.3d 1041, 1042 (N.Y. Sup. Ct. 2015).

Virginia: "A pleading for unjust enrichment must state that the defendant received benefits he should not justly retain, enriching the defendant at the plaintiff's expense or loss." *Whitehurst v. Cho*, No. 99231, 1992 WL 884510, at *1 (Va. Cir. Ct. Feb. 19, 1992). As discussed in Part VI.A, *supra*, Plaintiff Roberson fails to allege any actionable wrong, or that he lost money due to Clearview's conduct (or that Clearview has any money that belongs to him).

Illinois: "Unjust enrichment is not a separate cause of action under Illinois law." *Horist v. Sudler & Co.*, 941 F.3d 274, 281 (7th Cir. 2019). "[I]f an unjust enrichment claim rests on the same improper conduct alleged in another claim, then the unjust enrichment claim will be tied to this related claim—and, of course, unjust enrichment will stand or fall with the related claim." *Cleary v. Philip Morris Inc.*, 656 F.3d 511, 517 (7th Cir. 2011). Because the Illinois Plaintiffs fail to state a BIPA claim, *see* Parts II-V, *supra*, their derivative claim for unjust enrichment also fails.

VIII. The Claim for Declaratory Judgment and Injunctive Relief Should Be Dismissed

A claim for relief under the Declaratory Judgment Act, 28 U.S.C. § 2201 *et seq.* requires the existence of a justiciable case or controversy. *See Int'l Harvester Co. v. Deere & Co.*, 623 F.2d 1207, 1210 (7th Cir. 1980). Because Plaintiffs fail to state a claim in Counts One through Fifteen of the Complaint, Count Sixteen should likewise be dismissed because the Declaratory Judgment Act is not an independent source of jurisdiction.

CONCLUSION

For all these reasons, the Clearview Defendants respectfully request that the Court dismiss the Complaint with prejudice.

May 24, 2021

Respectfully submitted,

By: /s/ Lee Wolosky

Lee Wolosky (pro hac vice)
Andrew J. Lichtman (pro hac vice)
JENNER & BLOCK LLP
919 Third Avenue
New York, New York 10022-3908
Phone: (212) 891-1600
lwolosky@jenner.com
alichtman@jenner.com

Howard S. Suskin (ARDC No. 6185999)
Precious S. Jacobs-Perry (ARDC No. 6300096)
JENNER & BLOCK LLP
353 North Clark Street
Chicago, Illinois 60654
Phone: (312) 222-9350
hsuskin@jenner.com
pjacobs-perry@jenner.com

Floyd Abrams
Joel Kurtzberg
CAHILL GORDON & REINDEL LLP
32 Old Slip
New York, NY 10005
Phone: (212) 701-3000
fabrams@cahill.com
jkurtzberg@cahill.com

Attorneys for Defendants Clearview AI, In
Hoan Ton-That, Richard Schwartz, Rocky
Mountain Data Analytics LLC, and Thoma
Mulcaire

CERTIFICATE OF SERVICE

I certify that on May 24, 2021 I electronically filed the foregoing with the Clerk of Court using the CM/ECF system, which will then send a Notice of Electronic Filing to all counsel of record.

By: /s/ Lee Wolosky
Lee Wolosky